IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
ATHENS DIVISION

UNITED STATES OF AMERICA,	:	
	:	
v.	:	**CRIMINAL NO. 3:21-CR-9 (CAR)**
	:	
CEDDRICK DEMON MERCERY,	:	
	:	
Defendant.	:	
	:	

DEFENDANT CEDDRICK MERCERY'S MOTION TO SUPPRESS THE INSTAGRAM AND APPLE SEARCH WARRANTS

Defendant Ceddrick Mercery respectfully requests that the Court suppress (a) the breathtaking volume of digital information that the Government obtained from Cedric Mercery's Instagram account, which includes over well over 1,000 files of photos, videos, and communications and (b) the back-up copies of the entirety of Mr. Mercery's cellular telephones (and other Apple data) that were digitally stored in his Apple iCloud account.[1]

First, the Instagram warrant is unsupported by probable cause and is extraordinarily overbroad. Indeed, the face of the warrant reveals that it cannot meet the Fourth Amendment's particularity requirement. The warrant does not limit the agents' authority to seize and review the staggering volume of images, videos, and messages

[1] Instagram is a popular social media application that permits users to upload photos, send private message, post videos, and to "geo-tag" images (*i.e.*, to communicate geo-location information about uploaded content). *See, e.g.*, Instagram's Wikipedia entry for a summary of the incredible volume of data and information that Instagram retains about users. (https://en.wikipedia.org/wiki/Instagram).

obtained from Instagram.[2] It is as if a page is missing from the warrant. Such a glaring absence of particularity means that the Court should suppress the evidence, and the *Leon*-good faith exception cannot apply. Indeed, the absence of any information supporting the extreme scope of data requested by the warrant, as well as the lack of particularity in the warrant itself, rendered it unreasonable for any agent to rely on it.

Moreover, the Instagram affidavit recklessly misrepresented material information about a confidential source, namely, it omitted information that the source (a) has a criminal history and (b) is providing information to law enforcement and actively cooperating because of pending criminal charges. In short, the Court should suppress all evidence derived from the search and seizure of the contents of Mr. Mercery's Instagram account, including the fruits of any such searches.

Second, the Court should suppress the evidence derived from the search of Mr. Mercery's Apple iCloud. Unlike the facially deficient state Instagram warrant referenced above,[3] the Apple warrant **does** at least attempt to restrict the authority of the agents to "seize" only certain types of data.[4] But the agents **violated** the terms of the warrant,

---

[2] *Cf. Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant did not describe the items to be seized at all. In this respect the warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."); *Id*. at 559 ("We have clearly stated that the presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant.").

[3] A side-by-side comparison of the Instagram warrant with the Apple warrant reveals the Instagram warrant's facial deficiency. *Compare* Exhibit A (Instagram Warrant) *with* Exhibit B (Apple Warrant).

[4] *See In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 2013 WL 4647554, at *5 (D. Kan.

which only authorizes them to seize (or review) records created prior to September 23, 2020. Indeed, the records produced in discovery show that the iCloud back-up contains a wide swath of data from **prior to September 23, 2020**. Yet, the Government has made no effort to segregate that information or to limit the scope of its review. At a minimum, any digital records created prior to September 23, 2020 must be suppressed given the express terms of the warrant.[5] Moreover, Mr. Mercery is entitled to an evidentiary hearing to determine whether the agents "flagrant[ly] disregard[ed]" the terms of the warrant such that all the evidence, and the fruits thereof, must be suppressed. *Wuagneux*, 683 F.2d at 1354.

1. TFO Frost's affidavit and the Instagram warrant.

A. TFO Frost submitted a barebones affidavit to the Superior Court of Athens-Clark County in support of a warrant to search Mr. Mercery's Instagram account.

On November 12, 2020, FBI Task Force Officer Frost notified an Athens-Clarke County Police Department detective that he "would be seeking prosecution of Mercery through the federal system." See USAO-00095-96 (Report, attached hereto as Exhibit C.) (emphasis added). Despite his intention to bring the case federally, TFO Frost made the

Aug. 27, 2013) ("[A] warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject to seizure from those that are irrelevant.").

[5] "[T]he permissible scope of a search is governed by the terms of the warrant," *United States v. Wuagneux*, 683 F.2d 1343, 1352 (11th Cir. 1982), and "[o]nly items described in the search warrant may be seized." *United States v. Jenkins*, 901 F.2d 1075, 1081 (11th Cir. 1990); *United States v. Evaschuck*, 65 F. Supp. 2d 1360, 1368 (M.D. Fla. 1999) (suppressing evidence that was collected outside the scope of the warrant).

decision to obtain a warrant for Mr. Mercery's Instagram account from the Superior Court of Athens-Clarke County rather than a federal magistrate judge.

On November 16, 2020, TFO Frost presented an affidavit in support of the search warrant. Specifically, the affidavit alleged that Mr. Mercery engaged in criminal conduct on three dates: September 23, 2020, October 16, 2020, and October 26, 2020, all of which involved his possession of a firearm as a convicted felon. Notably, the affidavit does not identify any criminal conduct that Mr. Mercery engaged in that took place prior to **September 23, 2020**. *See* Exhibit D, Instagram Affidavit, at 2-3.

TFO Frost's affidavit confirms that he relied on information from a confidential source who apparently "provided a clothing description" of Mercery and who purported to know that Mr. Mercery's nickname was "Stunt." The affidavit explains that on October 21, 2020:

> [TFO Frost] was in contact with a confidential source of the Federal Bureau of Investigation. This source has provided information to Frost that has resulted in the seizure of illegal drugs. On this occasion the confidential source told Frost that it was aware **that an Individual it knows as Stunt** is wanted by law enforcement. The confidential source **further identified Stunt as Cedric Mercery**. The confidential source provided (***-***-**77) as Mercery's phone number. Additionally, the same source told Frost that Mercery was currently located in Rocksprings Homes and provided a clothing description. Officers went to the area of Rocksprings Homes and observed Mercery as he was described but were unable to take him into custody.

Instagram Affidavit, at 3 (emphasis added, phone number omitted).

While the agent affirmatively vouches for the informant's credibility by pointing out that he has provided information that "has resulted in the seizure of illegal drugs[,]" the affidavit omits any derogatory information about the source, namely, whether the

source has a criminal history, whether he is cooperating with law enforcement to obtain a favorable sentence or plea deal, or any other information that may negatively bear on his credibility.

Apparently relying on the confidential source's identification of Mercery and his nickname "Stunt"—but without further explaining how he identified Mercery's Instagram account—TFO Frost noted that he "reviewed Instagram Account name: https://instagram.com/stunt_devasi." His affidavit said that he "believes that [the] Instagram account name of stunt_devasi belongs to [Mercery]," that he is "familiar with Mercery" and that he has "observed that [Mercery] has multiple photos showing him under this account." Instagram Affidavit, at 4.

Although the affidavit does not say so, it appears that TFO Frost accessed certain publicly accessible portions of Mr. Mercery's Instagram account (since the affidavit provides some information about what TFO Frost saw in Mr. Mercery's account). Here's what the agent said (and didn't say) about what he saw on Mr. Mercery's Instagram account.

i. The affidavit's allegations about Instagram videos.

The affidavit says that "Mercery posted videos on his story of himself **discussing** committing acts of violence such as robbery to get money and illegal drugs" and that Mr. Mercery posted videos "with what appears to be large sums of money." Instagram Affidavit, at 4 (emphasis added). TFO Frost does not suggest that these videos depict Mr. Mercery carrying firearms, holding or brandishing weapons, or personally threatening any violence whatsoever. Likewise, the affidavit does not suggest that Mr. Mercery

discussed using guns, firearms, or weapons of any kind. And the affidavit does not identify the dates on which these videos were posted.

ii. The affidavit contains virtually no allegations about Instagram photos.

The affidavit contains no indication that the Instagram account contained any photos showing firearms, violence, narcotics, money, contraband, or criminal activity. Instagram Affidavit, at 4. The only allegation describing photos in the affidavit says that there were photos "showing" Mercery, but with no elaboration. *Id*.

iii. The affidavit does not identify any Instagram communications.

The affidavit does not identify any communications or written messages that Mercery sent or posted using Instagram. Nor does it identify any individuals with whom he is suspected to have been communicating with.

iv. While the affidavit says that there is probable cause to believe that there will be evidence of drug trafficking communications in the Instagram account, it says nothing about whether there is probable cause to obtain videos, photos, or any other Instagram data.

Despite the absence of any allegations establishing that Mr. Mercery is a drug dealer, purchaser, or user, TFO Frost explained that he believes, based on his "experience and training," that "individuals involved in the purchasing, use, and distribution of illegal drugs" use Instagram's **communication services** to traffic narcotics. *See* Instagram Affidavit, at 4. Not only are there no facts in the affidavit establishing probable cause to believe that that Mr. Mercery is an individual "involved in the purchasing, use, and distribution of illegal drugs"; the affidavit does not allege or suggest that Mercery's

Instagram account will contain videos, photos, or evidence showing that he possessed a firearm. Put differently, the affidavit does not allege or suggest that there is probable cause to believe that the **Instagram account** will contain any evidence about whether Mr. Mercery was a felon in possession of a firearm.

B. The search warrant compelled Instagram to produce the entire contents of Mr. Mercery's Instagram account, including videos, photos, and communications, going back to October 2019 with no restrictions on which items agents could seize.

Despite the fact that the warrant only identified criminal conduct in **September 2020 and October 2020**, and the fact that TFO Frost only believed that there was probable cause to access Instagram's messaging and communications services to find communications involving drug trafficking activity, a judge sitting the Superior Court of Athens-Clarke County issued an extraordinarily broad warrant directing Instagram to produce: (a) "[a]ll photographs and images in the user gallery for the account" **without any date restriction**; (b) all communications of messages received going back to **October 26, 2019** through October 26, 2020; (c) "[a]ll data and information that has been deleted by the user [sic] October 26, 2019 until October 26, 2020"; (d) "[a]ll user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other content [from] October 26, 2019 until October 26, 2020"; and more. *See* Instagram Warrant, at 1-2 (describing 18 categories of data). But the warrant contains no guidance on what data the agents may seize or properly review within the scope of the warrant.

The warrant notes that: "[t]here is now located certain instruments, articles,

person(s), or things, namely: [a list of 18 categories of Instagram records], [w]hich is being possessed as evidence of a violation of Georgia law, namely, O.C.G.A 16-11-131 Possession of a Firearm by a convicted felon[.]" Instagram Warrant, at 1-2. But **nothing in the warrant** purports to restrict the agent's authority to use the tremendous volume of Instagram data.

2. The Court should suppress the search and seizure of the contents of Mr. Mercery's Instagram account.

A. The Instagram warrant lacks particularity as there is nothing in the warrant that restricts, or authorizes, the Government to review the data produced by Instagram.

The warrant is facially overbroad and lacks particularity. For starters, the warrant only identifies the information that Instagram must produce to the law enforcement agents, namely, the 18 categories of data noted above. The warrant places no limit on what types of data that the Government may **seize** from that production of data. Nor does it expressly authorize the Government to seize that data. The warrant therefore lacks particularity. *Cf. Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant did not describe the items to be seized at all. In this respect the warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."); *Id*. at 559 ("We have clearly stated that the presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant."). In other words, the Government's review of the Instagram data has been, as a practical matter, warrantless.

Indeed, when the Department of Justice compels a third party, such as Instagram,

to produce email or other content via a search warrant, it generally attempts to comply with Federal Rule of Criminal Procedure 41 by creating a two-step process; the "search" involves a compelled production of broader categories of data from a third party, while the "seizure" involves the identification and copying of the data that the Government is authorized to review pursuant to the warrant. *See, e.g.*, *In re Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis*, 21 F. Supp. 3d 1, 8 (D.D.C. 2013) ("It is with the two-step procedure in Rule 41 in mind that the government has created the fiction that, although a great deal of information will be disclosed to it by Facebook, it will only 'seize' that which is specified in the warrant."). The U.S. Department of Justice has explained, in its manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,[6] how the two-step process under a Title 18, Section 2703 warrant works: "First, the warrant directs the service provider to produce all email [or other content] from within the specified account or accounts. Second, the warrant authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the **particularized 'items to be seized'** under the warrant." (emphasis added).

Here, there is no "items to be seized" part of the warrant. Because the warrant fails to identify (or particularize) which specific subset of records may be reviewed or "seized" by the Government, the warrant is facially deficient. Therefore, the Instagram

[6] The entire manual is publicly—accessible at this link: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

records, including all fruits derived therefrom, must be suppressed. *United States v. Leary*, 846 F.2d 592, 609 (10th Cir. 1988) ("We conclude that the government may not rely on the 'good faith' exception in this case and that all evidence seized under the Kleinberg warrant should be suppressed. We find the warrant so facially deficient in its description of the items to be seized that the executing officers could not reasonably rely on it.").[7]

B. **The Instagram warrant is grossly overbroad as to timeframe.**

TFO Frost's affidavit only identifies criminal conduct that took place over a two-month period: September and October 2020. The warrant, by contrast, compelled Instagram to produce all records **without a date restriction** when it came to "photographs and images in the user gallery for the account" and going back to October 2019—a year before any alleged criminal activity involving a firearm—for most of the

[7] *See also United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995) ("However, the warrant contained no limitations on which documents within each category could be seized or suggested how they related to specific criminal activity. By failing to describe with any particularity the items to be seized, the warrant is indistinguishable from the general warrants repeatedly held by this court to be unconstitutional."); *United States v. Rosa*, 626 F.3d 56, 61 (2d Cir. 2010) ("Rosa effectively argues that the warrant's authorization of an uncircumscribed search of his electronic equipment violated the Fourth Amendment's core protection against general searches because it provided the government with unrestrained access to electronic records of his daily activities and private affairs."); *In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 13-MJ-8163-JPO, 2013 WL 4647554, at *9 (D. Kan. Aug. 27, 2013) ("The warrants as currently proposed give the government virtual carte blanche to review the content of all electronic communications associated with the accounts and fail to adequately limit the discretion of the government-authorized agents executing the warrants. The absence of any limitations in the warrants on the government's review of the content of all email communications obtained from the Providers is in violation of the Fourth Amendment.").

other categories. That's too broad. *See, e.g.*, *United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) ("[T]he warrants should have requested data only from the period of time during which Moore was suspected of taking part in the prostitution conspiracy.") (emphasis added).

The warrant's failure to include an appropriate date restriction, tethered to the facts supporting probable cause, renders it overbroad and improper. *See, e.g.*, *United States v. Chen*, 17-CR-00603-BLF-1, 2020 WL 6585803, at *8 (N.D. Cal. Nov. 10, 2020) ("Courts in this district have found search warrants overbroad when the date range exceeds the reasonable scope of probable cause."); *United States v. Cerna*, CR 08-0730 WHA, 2010 WL 3749449, at *17 (N.D. Cal. Sept. 22, 2010) ("The date range of the search warrant, however, was overbroad and insufficiently particular."); *In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944, 952 (D. Alaska 2015) ("[T]he scope of the government's authority to search and seize under the warrant is not tailored to its probable cause showing. A warrant is overbroad if it expands the scope of the government's search beyond the places implicated by the probable-cause showing.").

Indeed, the affidavit doesn't even attempt to explain why the Instagram account would contain any relevant records from before September 2020. As the Eleventh Circuit noted in *Blake*, to avoid charges of being a "general warrant," warrants should only compel records related to the timeframe of the alleged criminal conduct. 868 F.3d at 974 ("With respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes

or customers. And the warrants should have requested data only from the period of time during which Moore was suspected of taking part in the prostitution conspiracy. Disclosures consistent with those limitations might then have provided probable cause for a broader, although still targeted, search of Moore's Facebook account. That procedure would have undermined any claim that the Facebook warrants were the internet-era version of a 'general warrant.'").[8]

Given that the affidavit covers criminal conduct within a narrow two-month period, the request to search for more than two months' worth of records is nothing more than the improper rummaging through private information. *Cf. United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Here, law enforcement knew that the evidence in

[8] *See also United States v. Matter of Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned*, 2:17-CM-3152-WC, 2017 WL 4322826, at *5 (M.D. Ala. Sept. 28, 2017), *on reconsideration sub nom. United States v. Matter of Search of Info. Associated with Fifteen Email Addresses Stored at Premises Owned , Maintained, Controlled or Operated by 1&1 Media, Inc.*, 2:17-CM-3152-WKW, 2017 WL 8751915 (M.D. Ala. Dec. 1, 2017) ("The Eleventh Circuit has recently noted that it is 'troubling' when searches of email accounts 'd[o] not limit the emails sought to emails sent or received within the time of [the suspect's] suspected participation in the conspiracy.' *United States v. Blake*, 868 F.3d 960, 973 n.7 (11th Cir. 2017). Other courts have likewise emphasized the importance of the time period for which the Government seeks digital information. *E.g., United States v. Hanna*, 661 F.3d 271, 287 (6th Cir. 2011) (upholding search warrant that was limited to 'the time period that the evidence suggested the activity occurred'); *In re Search of Google Email Accounts*, 92 F. Supp. 3d 944, 952 (D. Alaska 2015) (denying warrant application that 'would authorize the government to seize and search the entirety of the six Gmail accounts, even though the government has only established probable cause to look at a small number of emails within a narrow date range'); *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 72118, at *14 (E.D.N.C. Jan. 6, 2015) (concluding search warrant was overbroad since it 'offer[ed] nothing about the time frame of the offense' and instead sought all evidence 'since account inception'")).

support of probable cause in the affidavit revolved only around a three-month period in 1999; the authorization to search for evidence irrelevant to that time frame could well be described as 'rummaging'"). As a leading treatise put it, "an otherwise unobjectionable description of the objects to be seized is **defective** if it is broader than can be justified by the probable cause upon which the warrant is based." Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 4.6(a) General considerations, 2 Search & Seizure § 4.6(a) (6th ed.) (emphasis added).

Lastly, the warrant fails to limit its request for communications to particular individuals or suspected co-conspirators. *See Blake*, 868 F.3d at 974 ("With respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers."). Therefore, even if the warrant was properly limited as to time, it still lacked other appropriate protections that rendered it overbroad.

C. The "good faith" exception does not apply.

Here, the Government may not rely on the argument that the agents relied on the affidavit in good faith. *See, e.g.*, *United States v. Leon*, 468 U.S. 897, 922 (1984). First, the warrant was so facially deficient, and so at odds with U.S. Department of Justice practices, that the good faith exception does not apply. *Cf. Leary*, 846 F.2d at 609 ("We conclude that the government may not rely on the 'good faith' exception in this case and that all evidence seized under the Kleinberg warrant should be suppressed. We find the warrant so facially deficient in its description of the items to be seized that the executing officers could not reasonably rely on it."); *Groh v. Ramirez*, 540 U.S. 551, 558

(2004) ("In other words, the warrant did not describe the items to be seized at all. In this respect the warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). In other words, the officers cannot reasonably have presumed that this warrant was valid. The Court can suppress the Instagram search warrant on these grounds without an evidentiary hearing.

Second, the affidavit recklessly omitted information that would have (a) undermined the confidential source's credibility and (b) impacted the judge's ability to find probable cause to issue the warrant. As noted above, the only facts in the affidavit linking Mr. Mercery to the Instagram account (with the handle stunt_devasi) turn on information provided by the confidential source (relating to Mr. Mercery's nickname "Stunt" and Mr. Mercery's description). But the affidavit omitted information that undermines the credibility of the confidential source and would have undermined the judge's factual basis to make a probable cause finding.

The month before TFO Frost presented the Instagram search warrant affidavit, he submitted an affidavit in support of a geolocation warrant for Mr. Mercery's phone. *See* Geolocation Application and Affidavit attached hereto as Exhibit E. TFO Frost's affidavit in support of the application contained a paragraph about the confidential source that was virtually identical to the one he submitted in support of the Instagram warrant. But there was one difference. The geolocation affidavit noted that "**[s]aid source is also seeking to provide substantial assistance to law enforcement in connection with potential criminal charges**." Geolocation Affidavit, at 3 (emphasis added). But, for reasons that the Government has not explained, that paragraph was deleted and missing from TFO

Frost's affidavit in support of the Instagram warrant.

Given that the Instagram affidavit contains no explanation as to how TFO Frost would have known about Mercery's nickname "Stunt", his description, or his Instagram account (account name **stunt**_devasi) without relying on the confidential source,[9] information about the confidential source's credibility was material. *Cf. United States v. Glover*, 755 F.3d 811, 817 (7th Cir. 2014) ("The omission of that adverse information impaired the neutral role of the magistrate deciding whether to issue the warrant. As the government properly acknowledged at oral argument, such information is so essential to a witness's credibility that the same information regarding a government witness at trial would have to be disclosed to the defense as exculpatory material under *Brady v. Maryland*, 373 U.S. 83, 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972)."[10] In such circumstances, the good faith exception does not apply. *United States v. Martin*,

[9] Other than TFO Frost's statement that he is "familiar with Mercery," the affidavit does not allege that TFO Frost is able to independently identify Mr. Mercery's by his appearance. Nor does the affidavit allege that TFO Frost has ever seen Mr. Mercery in person, that he had previously seen photographs of Mr. Mercery, or whether his knowledge about Mercery's appearance is based on information from the source.

[10] *Cf. United States v. Novaton*, 271 F.3d 968, 987 (11th Cir. 2001) ("We find troubling Agent Lucas' apparent misrepresentations concerning the past cooperation of the informants involved in this case. Although the government maintains that there was an absence of proof concerning the agent's deliberateness or recklessness in making the misrepresentations, it is unclear how Agent Lucas could have made such statements of an affirmative character for which there was no basis without having acted either deliberately or recklessly. Accordingly, we will assume that this was a deliberate or reckless misrepresentation."); *United States v. Bradford*, 905 F.3d 497, 504 (7th Cir. 2018) ("Omitting [credibility] information deprives the magistrate of important data in the probable-cause calculus.").

297 F.3d 1308, 1312-1313 (11th Cir. 2002).

On the one hand, the Court could grant the motion to suppress without a *Franks* hearing (*i.e.*, a hearing to determine whether the information was omitted recklessly). *See Leon*, 468 U.S. at 915 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)). Indeed, a side-by-side comparison of the Instagram and Geolocation Affidavits confirms that the Instagram Affidavit omitted material information about the confidential source. But the proper course is to grant an evidentiary hearing so that Mr. Mercery can ascertain (a) whether there is additional negative information bearing on the source's credibility and (b) the reason why the information is missing from the Instagram affidavit.[11]

3. <u>The Court should suppress the search warrant for Mr. Mercery's iCloud data hosted by Apple.</u>

The information derived from the search of Mr. Mercery's Apple iCloud accounts should be suppressed. Unlike the facially deficient Instagram warrant referenced above,[12] the Apple warrant restricts the authority of the agents to "seize" only certain types of

[11] Mr. Mercery notes that the affidavit contains a number of other omissions, including (a) information indicating that Ms. Mitchell has retracted allegations related to the October 16, 2020 incident identified in the affidavit, (b) that Shownicia Hull, a witness the agent relied on in the affidavit, had herself committed drug and gun offenses, and is now under indictment by the U.S. Attorney's Office for the Middle District of Georgia (*See, e.g.*, *United States v. Shownicia Hull*, Case No. 3:21-CR-00035-CAR=CHW), and (c) other exculpatory information related to the September 2020 incident. Should the Court schedule a *Franks* hearing, Mr. Mercery respectfully requests an opportunity to question the agent about these facts and why they were omitted from the affidavit.

[12] A side-by-side comparison of the Instagram warrant with the Apple warrant reveals the Instagram warrant's facial deficiency. *Compare* Exhibit A (Instagram Warrant) *with* Exhibit B (Apple Warrant).

data.

Such restrictions were critical given the staggering volume of information that the Government sought in this case. Indeed, this was no mere search of an Apple iPhone. The Government obtained a warrant seeking all digital backups of every Apple device that Mr. Mercery owned or that were associated with his accounts, as well as data relating to virtually any and every Apple service he subscribed to. As the Supreme Court put it, "[m[odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life." *Riley v. California*, 573 U.S. 373, 403 (2014) (quotations omitted). But this warrant was even more intrusive as it sought all data associated with any iCloud backups of any of Mr. Mercery's phones, computers, and more.

Indeed, Attachment B to the affidavit contains a subsection entitled "Particular Things to be Seized" with a subsection, "I. Information to be disclosed by Apple," and a second subsection entitled "Information to be seized by the government[.]" Apple Warrant Attachment B, at 1-4. To that end, Attachment B.I. identifies a mind boggling array of digital data—including images of backups of Mr. Mercery's cellphone and computer data stored with Apple—that must be disclosed such as "the contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing"; the "contents of all emails associated with the account from September 23, 2020 to the date this warrant was authorized"; "[t]he content of all instant messages associate[d] with the account from September 23, 2020 to the date this warrant was authorized"; "[a]ll

records and information regarding locations where the account or devices associated with the account were accessed" and other data listed in B.I.

But page 4 of Attachment B contains a section entitled "[i]nformation to be seized by the government." Apple Warrant Attachment B, at 4. Attachment B imposes limits on what the agents were authorized to "seize," and one of the key limits was a hard date restriction. That is, the Government was only authorized to "seize" certain records created on or after **September 23, 2020**. That language is consistent with FBI SA Hipkiss's affidavit; he only describes criminal conduct that took place within the two-month window of September to October 2020. To that end, SA Hipkiss's affidavit represented to the U.S. Magistrate Judge that government authorized persons would only review the broad swath of Apple data "to locate the items described in Section II of Attachment B." *See* Affidavit in Support of an Application for a Search Warrant to Apple, attached hereto as Exhibit F at 14.

Yet, the records produced in discovery show that the agents have made **no effort** to segregate responsive records from non-responsive records. A cursory review of "the Apple iCloud Backup" records that the Government has produced in discovery shows that the Government seized large swaths of data created **before** September 23, 2020—contrary to the express terms of the warrant. Moreover, the FBI evidence log shows that the entirety of Mr. Mercery's iCloud data currently resides on a 500GB drive. *See* Evidence Log, attached hereto as Exhibit G. Based on the evidence log, it appears that the Government has made no effort to seize responsive records and segregate the non-

responsive information.[13]

Of course, "[t]he permissible scope of a search is governed by the terms of the warrant," *Wuagneux*, 683 F.2d at 1352, and "[o]nly items described in the search warrant may be seized." *Jenkins*, 901 F.2d at 1081; *Evaschuck*, 65 F. Supp. 2d at 1368 (suppressing evidence that was collected outside the scope of the warrant).

Therefore, the Court should suppress any and all records created before September 23, 2020 as (a) the warrant does not authorize agents to seize any such records, (b) SA Hipkiss represented to the U.S. Magistrate Judge that the government's review would be consistent with attachment B.II, and (c) there was no probable cause identified in the affidavit that would support viewing any records prior to September 23, 2020.

Second, the Court should grant a hearing so that Mr. Mercery can determine whether the Government has "flagrantly disregarded" the restrictions imposed by the warrant such that all the evidence obtained from Apple should be suppressed. *Wuagneux*, 683 F.2d at 1354.

Lastly, the Court should suppress the search of the Apple accounts because the affidavit in support of the warrant fails to establish probable cause for each and every Apple service that Mr. Mercery used. It is one thing to establish probable cause to believe that there may be some evidence on an iPhone. But it is quite another to assert that there is probable cause to search across every Apple service including iCloud Photo Library,

[13] Mr. Mercery notes that he has asked the Government to confirm whether it has separated responsive or non-responsive records from Apple iCloud account, including on June 7, 2021, and the Government has not confirmed whether it has done so.

iCloud tabs and bookmarks, iCloud Keychain, calendar entries, email accounts, instant messages, SMS messages, MMS messages, voicemails, videos, and for iOS backups of every phone or computer that Mr. Mercery ever used. As noted above, "an otherwise unobjectionable description of the objects to be seized is **defective** if it is broader than can be justified by the probable cause upon which the warrant is based." Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 4.6(a)General considerations, 2 Search & Seizure § 4.6(a) (6th ed.) (emphasis added). Therefore, the Court should suppress any evidence that is broader than the probable cause identified in the affidavit, which focused primarily on the potential for photos and videos. *See* Apple Search Warrant Affidavit, at 7.

CONCLUSION

Mr. Mercery respectfully requests that the Court suppress all evidence and any fruits derived from the search of Mr. Mercery's Apple and Instagram accounts as noted above.

Respectfully submitted this 7th day of September, 2021.

By: ***/s/ Kamal Ghali***
Kamal Ghali
Attorney for Defendant
BONDURANT MIXSON & ELMORE LLP
One Atlantic Center
1201 West Peachtree Street NW
Suite 3900
Atlanta, GA 30309
P: 404.881.4173
F: 404.881.4111
Email: ghali@bmelaw.com

CERTIFICATE OF SERVICE

I hereby certify that on today's date I electronically filed the Motion to Suppress with the Clerk of the Court using the CM/ECF system.

/s/ Kamal Ghali
Kamal Ghali
Attorney for Defendant
BONDURANT MIXSON & ELMORE LLP
One Atlantic Center
1201 West Peachtree Street NW
Suite 3900
Atlanta, GA 30309
P: 404.881.4173
F: 404.881.4111
Email: ghali@bmelaw.com